[ORAL ARGUMENT NOT SCHEDULED]
CASE NO. 22-5304

IN THE

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

JASON LEOPOLD,

Plaintiff-Appellant,

v.

J. THOMAS MANGER, *et al.*,

Defendants-Appellees

BRIEF OF APPELLANT JASON LEOPOLD

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

JEFFREY LIGHT, D.C. BAR #485360
Law Office of Jeffrey L. Light
1629 K Street, N.W.
Suite 300
Washington, DC 20006
(202) 277-6213
Jeffrey@LawOfficeOfJeffreyLight.com

Dated: April 18, 2023

Counsel for Plaintiff-Appellant

CERTIFICATE AS TO PARTIES, RULING, AND RELATED CASES

A. Parties and Amici

1. All parties, intervenors, and *amici curiae* who have appeared before the district court: Plaintiffs Jason Leopold and BuzzFeed, Inc., and Defendants Yoganada Pittman, J. Thomas Manger, and Michael Bolton.
2. There were no *amici curiae* or intervenors in the district court proceedings.
3. All persons who are parties, intervenors, and *amici curiae* appearing in this Court: Appellants Jason Leopold and Appellees J. Thomas Manger and Ronald Gregory. There are no intervenors or *amici curiae* in this case.

B. Rulings Under Review

The ruling at issue on appeal is the district court's [28] Order granting Defendant's Motion to Dismiss for Lack of Subject Matter Jurisdiction and denying Plaintiffs' Cross Motion for Summary Judgment. (JA-69.)

C. Related Cases

This case has not previously been before this or any other court. Counsel is not aware of any related cases currently pending in this or any other court that may be considered related for purposes of this rule.

/s/ Jeffrey Light

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

GLOSSARY OF ABBREVIATIONS

IG	Inspector General
OIG	Office of Inspector General
SAR	Semiannual Report
USCP	United States Capitol Police

JURISDICTIONAL STATEMENT

The district court possessed subject matter jurisdiction pursuant to 28 U.S.C. § 1361. This Court possesses jurisdiction pursuant to 28 U.S.C. § 1291.

Final judgment was entered by the district court in this case on September 20, 2022. (JA-69.) Jason Leopold filed his Notice of Appeal on November 18, 2022. (JA-95.)

STATEMENT OF ISSUES

The questions presented for review are:

1. Is there a common law right of access to U.S. Capitol Police Directives or portions of Directives that do not constitute "security information" as that term is defined under 2 U.S.C. §1979?

2. Is there a common law right of access to U.S. Capitol Police Office of Inspector General Semiannual Reports, Inspector General audits, and other reports?

3. Is there a statutory right of access to U.S. Capitol Police Office of Inspector General audits and reports which recommend corrective action?

STATUTES AND REGULATIONS

Pertinent statues and regulations are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

Plaintiff-Appellant Jason Leopold, then a Senior Investigative Report at BuzzFeed News,[1] requested that the U.S. Capitol Police (USCP) and its Inspector General (USCP IG) provide him with six categories of records, invoking his right of access under the federal common law. (JA-25-JA-26.) As relevant to this appeal, Mr. Leopold's request sought Inspector General Semiannual Reports; Inspector General reports, including audits; and USCP Directives. (JA-26.) After the USCP and USCP IG refused to provide Mr. Leopold with these records, he and his then-employer BuzzFeed News filed suit against Yogananda Pittman, Acting Chief of the USCP, and Michael Bolton, USCP IG. (JA-6.) Mr. Leopold and BuzzFeed News asserted a common law right of access to all three types of records at issue in this appeal and a statutory right of access to the USCP IG records. (JA-8-JA-9.)

The parties filed cross-motions for summary judgment. (JA-3-JA-4.) The district court denied the plaintiffs' cross-motion for summary judgment and, construing the government's motion for summary judgment as a motion to dismiss for lack of subject matter jurisdiction, granted the government's motion. (JA-69.) This timely appeal followed. (JA-95.)

[1] Mr. Leopold is currently a Senior Investigative Reporter at Bloomberg News.

SUMMARY OF ARGUMENT

The common law right of access applies to all three branches of government and helps ensure that the public can keep a watchful eye on the workings of public agencies. *Wash. Legal Found. v. United States Sentencing Comm'n*, 89 F.3d 897, 903, 905 (D.C. Cir. 1996) ("*WLF II*"). At issue in this case are two groups of records requested by Mr. Leopold which contain information that, if released, would promote public oversight of the working of the USCP by shedding light on agency policies and procedures, as well as the USCP OIG's documentation of agency waste, fraud, and abuse. The district court incorrectly allowed the government to keep all of these records secret in their entirety.

A. USCP Directives

The first group of records at issue in this case are USCP Directives, a set of documents embodying the agency's official policies and procedures on a wide variety of topics. (JA-28-29.) Of the Directives at issue in this case, a USCP Document Review Team determined that 65 must be withheld because they constitute "Security Information" under 2 U.S.C. § 1979. (JA-23.) The district court concluded that each of these Directives was properly designated as Security Information. (JA-85.) Accordingly, the district court found that as to these Directives, the common law right of access was preempted by 2 U.S.C. § 1979 and conducted no further analysis. (JA-86.) As to the Directives which were not

designated as Security Information by the USCP Document Review Team, the district court found that these documents do not meet the definition of a "public record" and that, in any event, they were properly withheld because government's interest in secrecy outweighs the public's interest in disclosure of the Directives. (JA-86-JA-87.)

In holding that the Directives designated by the USCP Document Review Team as constituting Security Information were correctly designated as such, the district court based its conclusion solely on the titles of a handful of Directives and the agency declarant's categorical assertion of harm that "could" arise from disclosure of hypothetical Directives. (JA-85). This evidence was not sufficient to establish that the Security Information designations were proper as to each and every Directive. Without an index of the type prescribed by this Court in *Vaughn v. Rosen*, 484 F.2d 820, 827 (D.C. Cir. 1973) or some other description of how the particular Directives designated as Security Information would meet the statutory elements of that term, the district court had an insufficient factual basis for its decision.

Further, the district court erred by evaluating the Directives as a whole in determining whether they constitute Security Information, rather than determining whether particular information within each Directive constituted Security Information. The use of the term "security information" in the statute indicates that

Congress was concerned with disclosure of information, not documents. However, the government's declarations did not make any attempt to correlate the elements of the statutory term "security information" with particular portions of the Directives, and the district court did not consider whether portions of the Directives could be segregated and released.

For the remaining Directives, the district court erred in concluding that they do not constitute public records because they are merely preliminary material. USCP Directives are not preliminary material because they have "legal significance, broadly conceived." *WLF II*, 89 F.3d at 905. They are binding on the agency and its employees, and there are legal consequences if employees violate them. The Directives also do not bear the indicia of preliminary material – they are not drafts, personal notes, or raw thoughts of an agency employee. Instead, they represent final statements of policy and practice on issues within the purview of the agency. The Directives also follow the formalities of official actions, including being printed on agency letterhead, indicating which previous policies are superseded or repealed, and bearing the signature of the Chief of Police acting in their official capacity to promulgate the Directives.

The district court concluded that the Directives are "preliminary" because they are relied upon by agency officials in making decisions. (JA-88.) Under this rationale, however, documents that are undisputedly public records would be

considered "preliminary" and therefore not public records. For example, legal briefs are relied upon by judges in issuing decisions in cases and are therefore "preliminary" in the sense that the district court used the term. However, legal briefs are public records precisely *because* they are relied upon by a judge in making an official decision. This Court's case law teaches that the relevant distinction between preliminary and non-preliminary material for purposes of the common law public right of access is whether the material has legal significance, broadly conceived. Neither legal briefs nor the Directives are preliminary because both have legal significance and are relied upon by officials in making official decisions.

Although the district court concluded that the Directives are not public records because it considered them to be preliminary material, it held in the alternative that the Directives should not be released because the government's interest in secrecy outweighs the public's interest in disclosure of the Directives. The district court's decision must be reversed because there was insufficient evidence in the record to support its conclusion as to the balancing of interests for each and every Directive at issue. While many of the Directives involve substantive law enforcement matters affecting members of the public, the district court nevertheless dismissed the significance of the Directives *in toto* as concerning mere administrative matters. (JA-90.) Thus, the district court erred in considering the public's interest

in disclosure. The district court also erred in accepting the government's generic and categorical assertion of harm from disclosure where the harm, if any, would vary significantly based on the subject matter of each Directive. The only evidence in the record specific to the harm that might arise from disclosure of a particular Directive was the title of each Directive. (JA-28-29.) However, the titles of many of the Directives are vague as to the subject matter involved, while other titles suggest that the subject matter is far removed from anything that would be harmful if disclosed. (JA-28-29.)

Finally, the district court abused its discretion by failing to consider whether portions of the Directives could be segregated and released. The Directives are structured into discrete sections such that even for Directives that involve sensitive topics, portions of the Directives could be released to the public without causing harm sufficient to outweigh the public's interest in disclosure. (JA-30-37.)

B. Office of Inspector General Reports and Audits

The second group of records at issue in this case are USCP Office of Inspector General (OIG) reports and audits. The district court concluded that all of the OIG reports and audits at issue in this case constitute Security Information under 2 U.S.C. § 1979. (JA-85.) Therefore, it did not reach the question of whether part or all of these records could be released under the common law right of access. (JA-

83.) The record does not support the conclusion that all USCP OIP reports and audits are Security Information.

The USCP OIG conducts a wide range of activities touching on virtually every aspect of the USCP's operations. 2 U.S.C. § 1909(c)(3)(A). As a result, its reports and audits could involve subject matters that range from highly sensitive security matters to more prosaic administrative issues. However, the degree of sensitivity involved with any of the particular reports or audits at issue in this case is unclear because the government did not submit a list of titles or description of the subject matters of any of the reports and audits. The government also did not describe how the OIG audits and reports are structured or explain why any sections that constitute Security Information could not be redacted, with the remaining portions released.

From the little information that is publicly available about the subject matter and structure of the audits and reports, it appears that at least some of the USCP OIG records at issue in this case are similar to those released by other intelligence and law enforcement agencies. The fact of the release by these other agencies as well the nature of the information contained therein suggest that not all of the records at issue in this case constitute Security Information, much less that all portions of all records at issue constitute Security Information. While it is unclear what differences there might be between audits and reports prepared by different

agency IGs on the same topic, what is clear is that the record lacks a *Vaughn*-like index or other description of the subject matter of each of the OIG records at issue. Without such information, the district court did not have a factual basis to affirmatively conclude that the OIG audits and reports at issue were categorically exempt from disclosure as Security Information.

In addition to asserting a common law right of access, Mr. Leopold asserted a statutory right of access to certain OIG material pursuant to 5 U.S.C. App. 3 § 4(e)(1), which requires that a document making a recommendation for corrective action be posted to the website of the Office of Inspector General within three days. The district court rejected this argument on the grounds that the public posting requirement for all Inspectors General offices, which was added until 2016, did not specifically mention that it would apply to the USCP OIG, which was established by a separate law in 2005. (JA-93.) The district court's conclusion that the public posting requirement does not apply to the USCP OIG was erroneous. Under the plain language of the statute, the USCP OIG "shall carry out the same duties and responsibilities . . . under the same terms and conditions which apply" to other Inspectors General. 2 U.S.C. § 1909(c)(1). Further, a recent amendment to 2 U.S.C. § 1909(c)(1) clarifies that this language applies to the duties and responsibilities of the other Inspectors General as they exist now, as opposed to the duties and responsibilities as they existed at the time the USCP OIG was created.

The district court's reliance on the "reference canon" of statutory construction, as recently articulated by the Supreme Court in *Jam v. Int'l Fin. Corp.*, 139 S. Ct. 759 (2019) does not compel a different result. As recognized by several other federal circuit courts of appeal, that canon of construction applies only where the language of the statute is ambiguous on its face, which is not the case here. Further, the "same duties and responsibilities" and "same terms and conditions" language in the statute at issue here is similar to the "same immunities" language which the Supreme Court found in *Jam* to incorporate any subsequent amendments to the referenced statute.

For the foregoing reasons, this Court should reverse the district court's order dismissing the First Amended Complaint for lack of jurisdiction and remand for further proceedings.

ARGUMENT

I. The district court erred in concluding that there is no common law right of access to any of the non-Security Information U.S. Capitol Police Directives.

A. Standard of review

The district court construed the government officials' Motion for Summary Judgment as a motion to dismiss for lack of subject matter jurisdiction pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure and granted the motion. (JA-69.) This Court "review[s] a district court's Rule 12(b)(1) dismissal *de novo*."

Allaithi v. Rumsfeld, 753 F.3d 1327, 1329 (D.C. Cir. 2014). Insofar as the district court reached the merits of the requesters' common law right of access argument, this Court reviews *de novo* whether a document is a public record. *Cf. CNN, Inc. v. FBI*, 984 F.3d 114, 117 (D.C. Cir. 2021). However, the ultimate disclosure decision is reviewed under an abuse of discretion standard. *Wash. Post v. Robinson*, 935 F.2d 282, 288 n.7 (D.C. Cir. 1991).

B. Non-Security Information Directives are public records.

For purposes of the common law right of access, this Court has defined a "public record" as "a government document created and kept for the purpose of memorializing or recording an official action, decision, statement, or other matter of legal significance, broadly conceived." *WLF II*, 89 F.3d at 902. Mr. Leopold argued to the district court that the non-Security Information Directives (*i.e.*, USCP Directives that do not contain "Security Information" as that term is defined in 2 U.S.C. § 1979) were "created and kept" to "memorializ[e] or record[]" "official . . . statement[s]" because their purpose is to set forth official agency policies and procedures. (R.21 at 3.) Mr. Leopold argued in the alternative that the Directives "memorializ[e] or record[]" the "decision" of the Chief of Police adopting the policies and procedures contained in the Directives. (R.21 at 3.) Finally, Mr. Leopold argued that the Directives have "legal significance" both because they are

binding on employees of the Capitol Police and also because they represent the official policies and procedures of the agency. (R.21 at 7-8.)

The district court did not determine whether the Directives were created and kept to memorialize or record an official "statement"; whether the Directives were created and kept to memorialize or record decisions of the Chief of Police to adopt those policies and procedures; whether the Directives can be said to have legal significance because they are binding on employees of the Capitol Police; or whether the Directives can be said to have legal significance because they represent the official policies and procedures of the agency. Instead, the district court concluded that the non-Security Information Directives at issue are not public records because they "amount to preliminary material" and "concern only the sort of administrative matters internal to the [USCP]" that do not constitute public records. (JA-88) (alteration in original). The district court erred in both lines of reasoning.

First, the district court incorrectly determined that the Directives, which are final, legally binding statements of agency policy, are merely "preliminary material" and therefore not public records. Second, the district court erred in concluding that the non-Security Information Directives concern only "administrative matters internal to the [USCP]" (JA-88) (alteration in original). However, even if the non-Security Information Directives concern only

administrative matters internal to the USCP, the district court was incorrect in concluding that these sorts of records are categorically excluded from the definition of "public records."

i. The Directives are not merely preliminary material.

This district court failed to grapple with the arguments made by Mr. Leopold, described above, as to why the Directives memorialize official actions or statements of legal significance. Instead, it reasoned that material is "preliminary," and therefore not a public record, if it "may be consulted to guide the action of [agency] personnel" and "may only eventually lead to an official action." (JA-88.) Under this reasoning, a brief and appendix submitted by a party in a judicial proceeding would not be public records because they are "preliminary material" in the sense of being "consulted to guide the action" of a judge and may "only eventually lead to an official action." However, a brief and appendix submitted by a party in a judicial proceeding are public records precisely *because* they are intended to be consulted to guide the action of a judge and eventually lead to an official action. *MetLife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 668 (D.C. Cir. 2017); *CNN*, 984 F.3d at 118 ("If the goal in filing a document is to influence a judge's decisionmaking, the document is a judicial record.")

In the context of the common law public right of access, what differentiates a brief submitted by a party in a judicial proceeding (which is a public record) from

the preliminary notes of a government auditor (which are not public records) is whether the writing was created or kept to memorialize a "matter of legal significance."[2] *WLF II*, 89 F.3d at 906. For example, the following materials do not constitute public records because they were not created to memorialize an official action or statement, lack legal significance, or both: "the report of a blood test provided in support of an application for a marriage license, the job application of a would-be government employee, a government auditor's preliminary notes used in the preparation of an official report, or a cover memorandum circulated with a copy of an official report or study." *Id.* at 905-06.

Although no binding case law since *WLF II* has elaborated on the issue of what constitutes an "official" action or statement of "legal significance," Judge Henderson's concurrence in *Judicial Watch, Inc. v. Schiff*, 998 F.3d 989 (D.C. Cir. 2021) ("*Judicial Watch II*") is instructive on these issues. In *Judicial Watch II*, this Court considered an appeal in which the same district court judge who presided over the present case held that the issuance of the requested subpoena was "a preliminary step to gather information pertinent to the Committee's task of deciding whether to recommend impeachment of the President and thus the

[2] This Court has explained that its definition of a public record subject to the common law right of access should be understood as being "consistent with the federal cases holding that documents and exhibits filed with or introduced into evidence in a federal court are public records." *WLF II*, 89 F.3d at 906.

subpoenas do not qualify as public records subject to the common-law right of public access." *Judicial Watch, Inc. v. Schiff*, 474 F. Supp. 3d 305, 315-16 (D.D.C. 2020) ("*Judicial Watch I*"). The panel majority did not reach the question of the common law right of public access, but Judge Henderson concluded in her concurrence that the "district court was plainly incorrect" in finding the subpoenas were preliminary and do not fall within the definition of a public record. *Judicial Watch II*, 998 F.3d at 995 (Henderson, J., concurring). Judge Henderson reasoned that the subpoenas have "independent legal significance" and therefore are not preliminary because "failure to comply with a Congressional subpoena may result in contempt proceedings whether or not the Committee ultimately takes action." *Id.* at 995-96.

The USCP Directives likewise have independent legal significance and therefore are not preliminary. USCP Directive 2053.013 ("Rules of Conduct"), Rule A3: "Compliance with Directives," explicitly states, "Employees are required to obey all Departmental . . . Directives[.]" (JA-30.) Failure to comply with the Directives may result in discipline against an officer whether or not the USCP ultimately takes any other action. *See Breiterman v. United States Capitol Police*, Civil Action No. 16-893 (TJK), 2020 U.S. Dist. LEXIS 162663, 2020 WL 5291991 (D.D.C. Sep. 4, 2020) (USCP disciplined officer for violation of directive); *Moran v. United States Capitol Police*, 82 F. Supp. 3d 117 (D.D.C.

2015) (same); *Anyaso v. United States Capitol Police*, 39 F. Supp. 3d 34 (D.D.C. 2014) (same). Further, the Directives have independent legal significance in that their validity can be subjected to judicial review, regardless of whether any actions are taken pursuant to the Directives. *See United States Capitol Police v. Office of Compliance*, 908 F.3d 776 (Fed. Cir. 2018) (considering various directives under collective bargaining agreement).

Judge Henderson's concurrence in *Judicial Watch II* also explained that the subpoenas at issue in that case constituted "official action" because they "were issued in accordance with House Rules," "issued on the official letterhead of the Congress of the United States," and were "signed by the chairmen of three House committees." 998 F.3d at 996. The Directives at issue in this case represent official actions for similar reasons. The Directives were issued on official USCP letterhead by the Chief of Police in their official capacity as chief executive officer of the USCP. (JA-30.) The subject matter of the Directives demonstrates that they are "official" in that they "reflect the USCP's internal policies, rules, protocols, and guidance for USCP personnel on a variety of subjects[.]" (JA-24.) The issuance of the Directives is also an activity within the scope of the Capitol Police's mission–

"polic[ing] the United States Capitol Buildings and Grounds under the direction of the Capitol Police Board[.]" 2 U.S.C. § 1961(a).[3]

As in *Judicial Watch I*, the district court in this case sidestepped the dispositive issue— whether the records were "created and kept for the purpose of memorializing or recording an official action, decision, statement, or other matter of legal significance, broadly conceived." *WLF II*, 89 F.3d at 902. The district court in this case did not explain if or why it thought that the non-Security Information Directives do not memorialize or record "official . . . statement[s.]" *Id.* The district court also did not explain if or why it thought that the non-Security Information Directives do not memorialize or record the "official . . . decision," *id.*, of the Chief of Police to issue the Directives. Finally, the district court did not analyze the binding nature of the Directives in determining that they lack "legal significance," *id.*

The Directives are also not properly characterized as merely preliminary material because they do not bear the indicia of preliminary material outside the scope of a public record. Particularly instructive on this issue is the common law public right of access in California.[4] Examples of preliminary materials that do not

[3] This stands in contrast to the public body at issue in *WLF II* which had "a very limited mission, namely, to recommend sentencing guidelines to the Sentencing Commission." 89 F.3d at 906.

[4] California case law is particularly instructive because these "informal and preliminary writings" are "essentially the same" category of material that this

constitute public records subject to a right of access to California common law include "initial drafts," "memoranda," "critical analyses of others' work," "preliminary drafts," "personal notes," and "rough records." *Copley Press, Inc. v. Superior Court*, 6 Cal. App. 4th 106, 114 (1992). These materials are preliminary because, by their very nature, they "are tentative, often wrong, and sometimes misleading." *Id.* Their purpose is "to extract raw and immature thoughts from the brain to paper, so that they can be refined and corrected." For example, a "judge's personal bench notes are constructed so as to remind him, in his personal fashion and not in a form digestible by the public, of the aspects of the case he thought important." *Id.*

The non-security information Directives at issue in this case are not analogous to these preliminary documents. They do not represent the personal notes or raw, immature thoughts of the Chief of Police, but are instead binding rules that must be followed. They are intended to be digested by all agency employees and are not rough or tentative drafts. Rather, they represent final statements of agency policy. *See Judicial Watch, Inc. v. United States DOJ*, 20 F.4th 49, 54 (D.C. Cir. 2021) ("A document is predecisional if it was generated *before* the adoption of an agency policy") (emphasis added, internal quotation marks omitted).

Court held in *WLF II* to be "pre-decisional" or incidental to official action. *Sander v. State Bar of Cal.*, 58 Cal. 4th 300, 319, 321 (2013).

Moreover, "[a] key feature under . . . the 'predecisional' . . . criteria is the relation between the author and recipients of the document. A document from a junior to a senior is likely to reflect his or her own subjective opinions and will clearly have no binding effect on the recipient. By contrast, one moving from senior to junior is far more likely to manifest decisionmaking authority and to be the denouement of the decisionmaking rather than part of its give-and-take." *Access Reports v. Dep't of Justice*, 926 F.2d 1192, 1195 (D.C. Cir. 1991). Here, the Directives are from the Chief of Police to the police force setting forth official agency policies and procedures. They are not an invitation to officers to engage in back-and-forth policymaking discussions with the Chief of Police.

Still further, many of the Directives are not predecisional because they do not relate to a definable decisionmaking process. *Paisley v. CIA*, 712 F.2d 686, 698 (D.C. Cir. 1983) ("If there is no definable decisionmaking process that results in a final agency decision, then the documents are not pre-decisional"), *vacated in part on other grounds*, 724 F.2d 201 (D.C. Cir. 1984). The defendants and district court did not identify any particular decision to which the policies contained in the Directives are preliminary, and it is not obvious what final agency decision could possibly be involved with, for example, "Self-Contained Breathing Apparatus Inspection and Maintenance" (JA-29.)

ii. Even records concerning administrative matters internal to an agency can still qualify as public records.

The non-Security Information Directives do not all "concern" "administrative matters internal to the [USCP]," as the district court put it. (JA-88) (alteration in original). Certainly, *some* of the non-Security Information Directives concern administrative matters internal to the USCP. However, other non-Security Information Directives concern substantive law enforcement matters (*e.g.*, "Crime Scenes and Evidence"), direct interactions with the public (*e.g.*, "Communicating with the Deaf/Hard of Hearing during Arrests, Stops, and Contacts"), or both (*e.g.*, "Search of Persons"). (JA-28.)

Even if the district court's characterization of the non-Security Information Directives at issue here as "administrative" was apt, however, documents concerning administrative matters internal to an agency are not categorically excluded from the definition of a "public record." The district court posited that the non-Security Information Directives at issue in this case "concern only the sort of 'administrative matters internal to the [USCP]' that the D.C. Circuit has held not to be public records," citing *WLF II*. (JA-88.) However, the district court's truncated quote omitted a key fact about the documents at issue in *WLF II* – they were "*letters or memoranda* on administrative matters internal to the Advisory Group," *id.* at 900 (emphasis added). Generally, the purpose of creating a letter or memorandum is to communicate information, not to serve as a memorialization or

recording of any official action or matter of legal significance.[5] Thus, whether the letters or memoranda at issue in *WLF II* were "public records" did not turn on whether they were about administrative matters internal to the Advisory Group or substantive legal discussions about how the Sentencing Guidelines should be changed. Indeed, this Court held in *WLF II* that even the "memoranda . . . on policy matters," which were also at issue in that case, were not public records. *Id.*

The Directives, by contrast, are documents created and kept for the purpose of memorializing official agency policies and procedures and recording the Chief of Police's decision to adopt those policies and procedures. As a category of documents, they serve a fundamentally different purpose than letters or memoranda, regardless of whether they pertain to internal administrative matters[6] or policy matters. The Directives do not reflect an agency employee's personal thoughts, but are instead "evidence of the manner in which the business of that unit of government has been conducted," *WLF II*, 89 F.3d at 905, *quoting City of St. Matthews v. Voice of St. Matthews*, 519 S.W.2d 811, 816 (Ky. 1974), and therefore constitute public records. Indeed, it is difficult to image a set of documents that are

[5] To be clear, Mr. Leopold is not suggesting that every letter or memorandum is excluded from the definition of a public record. For example, a "memorandum opinion" issued by a court is created for the purpose of memorializing the reasoning for the court's decision.

[6] Of course, the subject matter of the documents may be relevant to weighing the public interest in the second step of the common law right of access inquiry, but it does not determine whether the documents are public records in the first place.

more clearly evidence of "the manner in which the business of" the Capitol Police has been conducted than the USCP's written policies and procedures, embodied in the Directives, which the agency and its employees have been following.

C. As to the non-Security Information Directives, the trial court abused its discretion in finding that the balancing of interests favors nondisclosure.

As the Supreme Court has held, "matters of substantive law enforcement policy . . . are properly the subject of public concern[.]" *United States DOJ v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 766 n.18 (1989). The district court recognized this general principle, but minimized its significance here by characterizing the non-security information Directives as being merely trivial administrative matters. (JA-89-JA-90.) The titles of these Directives, however, reveal a wide variation in the types of law enforcement policies at issue. Some are less likely to reveal matters of substantive law enforcement policies than others. *Compare* "Rayburn House Office Building Range" with "Bias-Based Profiling." (JA-28.) Among the non-Security Information Directives that relate to matters of substantive law enforcement policies, there is an especially great interest in disclosure of those Directives which involve interactions with members of the public. In addition to "Bias-Based Profiling," such Directives would include "Search of Persons" and "Conducting Preliminary Investigations." (JA-28.)

On the other side of the balance, the district court identified the need for government secrecy as being supported by the fact that the USCP labeled its non-Security Information Directives as "Law Enforcement Sensitive." (JA-89.) The district court noted that the designation "Law Enforcement Sensitive" is "widely used throughout federal state, and local law enforcement agencies to control and safeguard sensitive information," (JA-89) (internal quotation marks omitted) but as this Court has observed, the "Law Enforcement Sensitive" designation is vague and has no consistent meaning across agencies in terms of what information is considered sensitive. *Parhat v. Gates*, 532 F.3d 834, 853 (D.C. Cir. 2008); *Harmon v. Thornburgh*, 878 F.2d 484 (D.C. Cir. 1989); *Ameziane v. Obama*, 699 F.3d 488, 495 (D.C. Cir. 2010). As the designation "Law Enforcement Sensitive" pertains specifically to USCP information, it "indicates that such information should only be accessed by those with a need to know and should be reasonably protected from unauthorized disclosure." (JA-24.) Thus, while the designation by the USCP of information as "Law Enforcement Sensitive" represents a conclusion by the agency that distribution of the information should be restricted, it sheds no light on *why* the distribution of the information should be restricted.

Among the non-Security Information Directives, the degree of sensitivity that could plausibly be involved ranges from low or nonexistent (*e.g.*, "Budget Object Classification Codes" or "Roles, Authority, and Responsibilities of the Office of

Inspector General (OIG)") to potentially significant (*e.g.*, "Protective Body Armor.") (JA-28.) Accordingly, it was especially important for the district court to "balance the government's interest in secrecy against the public's interest in disclosure with reference to the contents of the *particular documents* at issue (as reflected in the *Vaughn* index) to determine whether [the plaintiff] has a common law right of access to those documents." *Wash. Legal Found. v. United States Sentencing Comm'n,* 17 F.3d 1446, 1452 (D.C. Cir. 1994) ("*WLF I*") (emphasis added). In conducting its balancing analysis in this case, the district court improperly mixed and matched between attributes of different non-Security Information Directives. While it is plausible that some non-Security Information Directives consist of nothing more than "trivial administrative matters" and others "reveal the methods, techniques, and responses that the USCP employs for Capitol Grounds security and could also increase the potential for individuals and groups that wish to disrupt, attack, or harm the Capitol or the Congress to do so," (JA-90) it does not follow that *both* of these attributes describe *every* non-Security Information Directive. Since the district court did not have before it a *Vaughn* index describing the contents of particular Directives, as required by *WLF I*, 17 F.3d at 1452, it was not in a position to properly conduct the balancing analysis required by this Court's case law. Had the district court had before it a proper *Vaughn* index, it may well have concluded that the public release of at least some

of the non-Security Information Directives is appropriate, just as many jurisdictions have concluded that the public release of similar law enforcement policy documents is appropriate. (JA-39-JA-40.)

Although the government provided a list of titles of Directives, this was not a satisfactory substitute for a *Vaughn* index. The list of titles, even combined with the government's declaration, does not fulfill the purposes of a *Vaughn* index because it lacks specificity as to what harm would arise from disclosure of which Directive. *Cf. King v. United States Dep't of Justice*, 830 F.2d 210, 224-25 (D.C. Cir. 1987) ("A withholding agency must describe *each* document or portion thereof withheld, and for *each* withholding it must discuss the consequences of disclosing the sought-after information") (emphasis in original). The purposes of a *Vaughn* index are "to permit adequate adversary testing of the agency's claimed right to an exemption" and enable "the District Court to make a rational decision whether the withheld material must be produced without actually viewing the documents themselves, as well as to produce a record that will render the District Court's decision capable of meaningful review on appeal." *Id.* at 218-19. The information contained in the record in this case does not enable adequate adversary testing or a rational decision by the district court. For example, the effects of public disclosure of the "Purchase Card Program" Directive are likely to be very different from the effects of disclosure of the "Use of Long-Range Acoustical Device

(LRAD)" Directive, but the government's categorical description of the harm that might result from public disclosure does not distinguish between these Directives.

Further, the government failed to distinguish between the different harms that might result from disclosure of different portions of a single Directive. This Court has held that in conducting a balancing analysis for public records, at least some of the *Hubbard* factors[7] should be applied to information within a public record, rather than the document as a whole, overruling the district court's decision to the contrary. *CNN*, 984 F.3d at 119. Where appropriate, portions of records for which the balance tips in favor of government secrecy can be redacted, with the rest released. *Leopold v. United States*, 964 F.3d 1121, 1133 (D.C. Cir. 2020).

Finally, the district court cited by way of analogy Exemption 2 of FOIA, which exempts from disclosure agency records that are "related solely to the internal personnel rules and practices of an agency." (JA-88.) However, most of the Directives at issue do not relate solely to *personnel* rules and practices in the sense of rules and practices dealing with employee relations or human resources. *See Milner v. Dep't of the Navy*, 562 U.S. 562, 570 (2011) ("An agency's 'personnel rules and practices' are its rules and practices dealing with employee relations or human resources.") Perhaps the Directive relating to "Grievance Procedure" could be construed as relating solely to personnel rules and practices, but the same

[7] *United States v. Hubbard*, 650 F.2d 293 (D.C. Cir. 1980).

cannot be said about the many non-Security Information Directives that relate to interactions with members of the public, such as "Search of Persons" and "Arraignment of Arrestees." Even internal policies with respect to personnel rules such as training and discipline, however, can greatly affect members of the public, sometimes in deadly ways. *See e.g.*, *Gaddis v. Redford Twp.*, 364 F.3d 763, 775 (6th Cir. 2004) ("[I]nadequate training procedures of the Cincinnati police department may have contributed to the shooting death of the plaintiff's suicidal, mentally ill decedent.") Given the potential for internal personnel rules and practices to have external impacts, the Supreme Court has held that "Exemption 2 is not applicable to matters subject to . . . a genuine and significant public interest." *Dep't of the Air Force v. Rose*, 425 U.S. 352, 369 (1976). Thus, to the extent that Exemption 2 of FOIA provides a useful analogy in the context of the common law right of access, the analogy counsels against withholding.

II. The district court erred in concluding that all material designated as "Security Information" fits within the statutory definition of that term.

Under 2 U.S.C. § 1979, Security Information may be released[8] by the USCP to another entity, including an individual, only if the USCP Board "determines in consultation with other appropriate law enforcement officials, experts in security

[8] Despite the apparently mandatory language of the statute, the USCP's declarant states that the USCP made a "discretionary release" of a Security Information Directive. (Joyce Decl. ¶ 7.)

preparedness, and appropriate committees of Congress, that the release of the security information will not compromise the security and safety of the Capitol buildings and grounds or any individual whose protection and safety is under the jurisdiction of the Capitol Police." The USCP Board has not authorized release of any Security Information at issue in this case. The question presented in this case, instead, is whether the requested material constitutes Security Information in the first place.

As used in 2 U.S.C. § 1979(b), "the term 'security information' means information that . . . is sensitive with respect to the policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response relating to Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds[.]" 2 U.S.C. § 1979(a)(1). In concluding that all material designated by the defendants as Security Information fits within the statutory definition of that term, the district court committed at least two errors. First, the district court improperly ruled that the designated documents constitute Security Information, rather than whether specific information contained within the documents constitutes Security Information. Therefore, reasonably segregable non-Security Information may have been improperly withheld. Second, the district court's conclusion that all of the documents at issue constitute Security Information was not supported by the record.

A. Segregability

Under 2 U.S.C. § 1979, the USCP may withhold "security information." Because the plain text refers to "security information" and not "documents containing security information," decisions on withholding should not be made on a document-by-document basis. Congress understands the difference between "information" and "documents" and chose here to focus on the withholding of information, not documents, as it did in the analogous context of FOIA.[9] *Cf. Mead Data Cent., Inc. v. United States Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977) ("The focus of the FOIA is information, not documents, and an agency cannot justify withholding an entire document simply by showing that it contains some exempt material.") Moreover, since this withholding statute is in derogation of the common law right of public access to congressional records, it should be construed narrowly. *Robert C. Herd & Co. v. Krawill*, 359 U.S. 297, 304 (1959) ("Any such rule of law, being in derogation of the common law, must be strictly construed, for no statute is to be construed as altering the common law, farther than its words import") (internal quotation marks omitted).

Although the withholding of information within documents can be accomplished through the familiar technique of redaction, *Rose*, 425 U.S. at 381,

[9] Although the current version of FOIA contains an explicit segregability provision, 5 U.S.C. § 552(b), and 2 U.S.C. § 1979 does not, segregability was a requirement under FOIA even before the explicit segregability provision was added in 1974. *Weissman v. CIA*, 565 F.2d 692, 697 (D.C. Cir. 1977).

the government offered no explanation as to why redaction of Security Information is not possible here, and the district court did not consider the issue. If this Court holds that Directives are or may be public records, the government should be required on remand to review the Directives it designated as constituting Security Information and indicate which *portions* of those Directives constitute Security Information.

B. The record does not support the conclusion that all of the Directives designated as Security Information were properly designated as such.

"The term 'security information' means information that . . . is sensitive with respect to the policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response relating to Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds[.]" 2 U.S.C. § 1979(a). Thus, information does not qualify as "security information" unless the information is (1) "sensitive" (2) "with respect to" one of the enumerated categories.[10] Information that is "sensitive" with respect to some other concerns, such as information which is politically "sensitive" does not qualify for

[10] Information will also not qualify as "security information unless the information is "obtained by, on behalf of, or concerning the Capitol Police Board, the Capitol Police, or any incident command relating to emergency response." 2 U.S.C. § 1979(a)(1). In this case, however, it is not disputed that all of the records meet this element.

withholding under the statute.[11] Nor does information that relates to one of the categories, such as policing, count unless the information is "sensitive." Had Congress intended for "security information" to include all information, regardless of sensitivity, it surely would not have included the word "sensitive" in the definition. *Cf. Zhen Nan Lin v. United States DOJ*, 459 F.3d 255, 262 (2nd Cir. 2006) (with respect to provision prohibition disclosure of certain information, "[t]he plain language of the regulation does not include any qualifiers like the word 'sensitive,' and we decline to read such a limitation into the regulation's text.")

Further, "security information" must involve "security." While the enumerated category of "policing" is potentially capacious, the enumeration of categories cannot extend the term "security information" beyond information that involves "security" because there is no reason to think that Congress intended to create such dissonance. *See Johnson v. United States*, 559 U.S. 133, 136 (2010). Thus, for example, even though an internal memorandum discussing potential media strategies for explaining a controversial policy is arguably sensitive with respect to policing, it is not sensitive with respect to security, and therefore would not be "security information."

[11] That is not to say that the information which is sensitive for other reasons that those listed in 2 U.S.C. § 1979 must be released. Information that is not Security Information, but nonetheless requires secrecy, may still be properly withheld under the second step of the balancing test for the common law right of access to records.

Applying this statutory construction to the Directives designated by the USCP Document Review Team as constituting "security information," the record does not support the district court's conclusion that all of these Directives were correctly designated as such. The district court held that "[g]iven the subject matter contemplated by these directives, defendants persuasively posit that if the 'sensitive law enforcement information contained in the security information directives' were to be made available for the public, it 'could unduly reveal the methods, techniques, and responses that the USCP employs for Capitol Grounds security and could also increase the potential for individuals and groups that wish to disrupt, attack, or harm the Capitol or the Congress to do so.' *See* OGC Decl. ¶ 12." (JA-85.) However, the conclusory statements of the government's declarant, viewed in light of the other record evidence, do not establish that all of the Security Information designations are correct with respect to every Directive so-designated, much less that every section of every Directive is Security Information.

First, the record contains only the titles of the Security Information-designated Directives and brief descriptions of the categories they fall into. While some of the titles of the Security Information-designated Directives indicate the subject matter with some degree of specificity (*e.g.*, "Staffing of Posts During Inclement Weather"), many give only a vague clue as to the subject matter (*e.g.*, "Change Management"). (JA-28-JA-29.) Attempting to apply the statutory definition of

"security information" to these vaguely worded titles is often impossible. Thus, the district court was not in a position to properly rely on the "subject matter contemplated by these directives" (JA-85) because not all of the titles revealed the subject matter.

Other titles appear to affirmatively establish that the subject matter of the Directive does not involve Security Information. It is difficult to see how the following Security Information-designated Directives involve policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response: "Retrieval of Archived Video," "Account Management," "Change Management," and "Self-Contained Breathing Apparatus Inspection and Maintenance." (JA-28-JA-29.) Likewise, it is difficult to see how the following Security Information-designated Directives, even if they involve one of the enumerated categories, could be considered sensitive: "Jurisdiction and Authority," "Recruit Officer Entry-Level Training Program," "Police Authority Shared with Other Law Enforcement Organizations." (JA-28-JA-29.) The following Directives, even if they met the other criteria, do not appear to involve any type of security at all: "Risk Management," "Telecommunications," "Congressional Pages," "Property and Asset Management." (JA-29.)

In reaching its conclusion that all of the Security Information-designated Directives were properly designated as such, the district court listed some

examples of Directives that are mostly, if not entirely, composed of Security Information. For example, the district court cited a few examples including "Responding to a Suicide Bomber: 10-100 S (Sam)" and "Building Evacuations" (JA-85.) The fact that these Directive are likely to be Security Information Directives does not justify the conclusion that "Jurisdiction and Authority," (JA-28) for example, is also a Security Information Directive. While the district court presumably intended its list of examples to be merely illustrative, its cherry-picked examples will only carry its analysis so far in justifying a conclusion that every single one of the Security Information-designated Directives was correctly designated.

To the extent that the district court reached its decision based on the declarations submitted by the government, those declarations are too vague and conclusory to support the district court's ultimate determination on the issue of whether each of the Security Information-designated Directives was properly designated.[12] A declaration must show *how* its conclusion was reached, and a brief

[12] Although this Court has often spoken of the need for non-conclusory declarations in the context of FOIA, the same principles apply here. "This lack of knowledge by the party seeking disclosure seriously distorts the traditional adversary nature of our legal system's form of dispute resolution. Ordinarily, the facts relevant to a dispute are more or less equally available to adverse parties. In a case arising under the FOIA this is not true, as we have noted, and hence the typical process of dispute resolution is impossible." Vaughn v. Rosen, 484 F.2d 820, 824-25 (D.C. Cir. 1973). Just as in a FOIA case, in this case the typical

mention of the subject matter of a document is insufficient. *Racing Enthusiasts & Suppliers Coal. v. EPA*, 45 F.4th 353, 359 n.3 (D.C. Cir. 2022) ("Its conclusory declaration does not explain with any specificity *how* the preamble's aside has made it choose between 'costly compliance and the risk of prosecution at an uncertain point in the future'") (emphasis in original); *S. of P.R. ex rel. Judiciary Comm. v. United States DOJ*, 823 F.2d 574, 585 (D.C. Cir. 1987) ("The information provided by the DOJ – consisting almost entirely of each document's issue date, its author and intended recipient, and the briefest of references to its subject matter – will not do.")

This Court has also explained that "[c]ategorical description of redacted material coupled with categorical indication of anticipated consequences of disclosure is clearly inadequate." *King*, 830 F.2d at 224. The declarations in this case are clearly inadequate because they merely couple a categorical description of the withheld material – "methods, techniques, and responses that the USCP employs for Capitol Grounds security" – with a categorical indication of the anticipated consequences disclosure – "increas[ing] the potential for individuals and groups that wish to disrupt, attack, or harm the Capitol or the Congress to do so." (JA-25.) There is no explanation as to *how* disclosure of the withheld methods, techniques, and responses that the USCP employs for Capitol Grounds security

---

process of dispute resolution is impossible as to the issue of whether information is security information.

would increase the potential for the anticipated harm. There is not even a brief mention of the subject matter of the Directives aside from what can be gleaned from the titles which, in some instances, is not much (*e.g.*, "Change Management"). Without a more detailed explanation, the district court could not have properly concluded that the withheld information was "sensitive."

The Joyce declaration also asserts only that disclosure "could" unduly reveal methods, techniques, and responses for security, and "could" increase the potential for individual and groups to disrupt, attack or harm the Capitol or Congress. (JA-25.) That is not enough. This Court has held that a declaration is not sufficient if it only alleges harms that "could" arise or what "may" be contained in a record. *Citizens for Responsibility & Ethics in Wash. v. United States DOJ*, 746 F.3d 1082, 1100 (D.C. Cir. 2014). Disclosure of almost any information held by law enforcement "could" reveal methods, techniques, and responses employed for security, and disclosure of almost any information at all – law enforcement or otherwise – "could" increase the potential for individuals to harm the Capitol or Congress.

The Joyce declaration's assertion as to what "could" be revealed by disclosure and what harms "could" arise are more sensible as to some Security Information-designated Directives than others. For some Security Information-designated Directives, there does not appear to be any logical or plausible connection at all

between the subject matter of the Directive and methods, techniques, and responses for security, or between the subject matter of the Directive and the potential for disruption, attack, or harm to the Capitol or Congress. For example, there is no obvious link between the subject matter of the Security Information-designated Directive "Jurisdiction and Authority" (JA-28) and any method, technique, or response for security. There is no apparent link between the subject matter of the Security Information-designated Directive "Account Management" (JA-29) and the potential for individuals and groups that wish to disrupt, attack, or harm the Capitol or the Congress to do so.

It may be that on remand the government is able to establish a rational link between each one of the Security Information-designated Directives and one of the enumerated categories and articulate a risk of harm.[13] As it stands, however, the government's declarations do not differentiate at all between the law enforcement methods and techniques that might be present in the "Congressional Pages" Directive and those that might be present in the "Air Threat Response Plan." (JA-

[13] Given the number of documents at issue, the government could potentially group some of the directives together into categories to avoid repetition. For example, the government might group several Directives together if they all share the same or similar cybersecurity techniques and the harm of disclosure for all of the Directives in the group is increasing the potential for Capitol Police computers to be infected with a computer virus. *Cf. Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 789 F.2d 64, 67 (D.C. Cir. 1986) (under FOIA, the "hallmark of an acceptable category" is "that it is *functional*; it allows the court to trace a rational link between the nature of the document and the alleged likely interference") (emphasis in original).

28.) Nor is there any differentiation between the harm that might arise from disclosure of "Antivirus and Malware Protection" as compared to the disclosure of "Self-Contained Breathing Apparatus Inspection and Maintenance." (JA-29.) Without these details, Mr. Leopold was not in a position to challenge, and the district court was not in a position to determine, whether these Security Information-designated Directives actually constituted Security Information.

The only other reference the Joyce declaration makes to the subject matter of the Directives or the potential harm that would arise from disclosure is the following statement: "As indicated by the Law Enforcement Sensitive designation on each page, these directives contain operational information that would reveal confidential sources and methods, investigative activities and techniques." (JA-24.) However, the fact that a "Law Enforcement Sensitive" designation appears on a Directive does not indicate that the Directive is Security Information because *every* Directive, whether or not it constitutes Security Information, is designated "Law Enforcement Sensitive." (JA-74.) While the government may address similar harms by category, its reliance on the "Law Enforcement Sensitive" reference "is not so much categorical as universal," *United States DOJ v. Landano*, 508 U.S. 165, 175 (1993). Because the Law Enforcement Sensitive designation is used to label *every* Directive, the government is requesting the Court to presume that disclosure of any Directive would reveal confidential sources and methods,

investigative activities, and techniques. This "sweeping presumption" does not "comport[] with common sense and probability." *Id.* (internal quotation marks omitted). The Directive "Rules of Conduct," for example, is stamped "Law Enforcement Sensitive" on every page, (JA-30-JA-37) but the government concedes that it does not contain Security Information (JA-28). Further, it is unclear what, if anything, in the "Rules of Conduct" makes the document "Law Enforcement Sensitive." It does not contain operational information that would reveal confidential sources and methods or investigative activities and techniques, and has in fact been publicly disclosed through official channels. (JA-30-JA-37.)

Turning to the issue of segregability, the Joyce declaration does not describe the structure of the Directives or explain how any Security Information is distributed through the Directives. However, a review of the few publicly released Directives reveal that at least some areas are unlikely to contain Security Information, such as "Authority and Coverage," "Definitions," and "Cancellation." (JA-30-JA-37.) Since the district court made no findings as to segregability, remand is appropriate for the district court to make such findings in the first instance. *Krikorian v. Dep't of State*, 984 F.2d 461, 467 (D.C. Cir. 1993).

C. The record does not support the conclusion that all OIG material is Security Information.

Mr. Leopold requested "semiannual reports summarizing the activities of the Office of the Inspector General for the period of 2015 forward" and "all other

Office of the Inspector General (OIG) reports, including any audits, for the period 2008 forward." (JA-26.) The first declaration of then-Inspector General Michael Bolton identified three types of reports that the OIG produces: (1) "a report at the conclusion of [an] audit or investigation"; (2) "semi-annual reports"; and (3) "annual . . . financial audit report[s] on the USCP's annual financial statements[.]" (JA-16.) The First Bolton declaration then provided hypothetical examples of what an OIG report "might" or "could" include. (JA-16.) In contrast to the Directives, the government did not even provide a listing of titles of the OIG reports that are responsive to Mr. Leopold's request.

i. Reports

The government's declarations are woefully inadequate to support a conclusion that each of the requested OIG reports constitutes Security Information. With respect to the first category of records produced by the OIG (reports at the conclusion of an audit or investigation), the lack of detail concerning the subject matter of the audits or investigations makes it impossible to determine whether each withheld report constitutes Security Information, much less that all reports categorically constitute Security Information. The reports cover diverse topics, some of which are more likely to be Security Information than others. For example, on the one hand, the First Bolton declaration refers to a hypothetical OIG report which "could" include "findings and recommendations regarding sensitive

posting locations for USCP officers and personnel in the Capitol building and on Capitol Grounds." (JA-16.) The subject matter of such a report suggests that it would contain information pertaining to the "physical security" of the Capitol or the gathering of "intelligence," 2 U.S.C. § 1979(a)(1). On the other hand, there is nothing in the record to suggest that the non-hypothetical "Performance Audit of the United States Capitol Police Training Services Bureau" (OIG-2016-07) (JA-65) relates to security or that it is sensitive with respect to any of the enumerated categories.

In reaching its conclusion that all of the OIG reports at issue are Security Information, the district court relied on the discussion in the First Bolton declaration of two hypothetical reports and the fact that some of the OIG's work involves national security and law enforcement sensitive matters. (JA-86.) Even if the district court's analysis referred to real (as opposed to hypothetical) reports and those reports constituted security information, it does not follow that every OIG report constitutes security information. These examples, taken "in consideration" of the nature of the OIG's work (JA-86), shed no light on how, for example, a performance audit of the Training Services Bureau is sensitive with respect to one of the enumerated categories. Because the OIG investigates a wide range of issues, including potential "violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the

public health and safety," 2 U.S.C. § 1909(c)(3)(A), the district court's categorical treatment of the OIG reports improper.

Further, the offices of Inspectors General for other agencies which deal with national security information, including the National Security Agency (NSA), make publicly available reports concerning a variety of topics including waste of government funds.[14] If a 47-page audit of the NSA's travel program can be posted to that agency's website without revealing any sensitive information, it is unreasonable to believe that the USCP's audit of its own travel card program (OIG-2019-12) is so sensitive that not a single page can be safely released to the public.[15]

On the issue of segregability, the structure of OIG reports, including those pertaining to security issues, is amenable to redaction. Indeed, the reports are specifically designed to be segregable. As one prior USCP IG explained to Congress, "[I]n accordance with OIG's reporting protocols, *the Executive Summary; Objectives, Scope and Methodology*; and *Body* of the report must all

---

[14] *See e.g.*, "Audit of the Agency's Travel Program," (47 pages), *available at* https://oig.nsa.gov/Portals/71/Reports/Reviews/Final%20Travel%20Audit%20AU%2018%200003%20Public%20Release.pdf?ver=2019-03-01-144443-310; "Audit of Cost-Reimbursement Contracts" (54 pages), *available at* https://oig.nsa.gov/Portals/71/Reports/Reviews/Cost_Reimb_Report.pdf?ver=Ag-RBUeqikr50aRzgALDgg%3d%3d

[15] *See* https://www.uscp.gov/sites/uscapitolpolice.house.gov/files/wysiwyg_uploaded/Peer%20Review%20Report%20%282019%29.pdf (listing USCP OIG reports).

stand alone and can be read as separate documents." (JA-61) (italics in original). An example of a security-related document that can be segregated along these lines is the public Flash Reports made available by Congress which pertains to the events surrounding the January 6, 2021 takeover of the U.S. Capitol. (JA-51.) On the cover page is the title "Flash Report: Operational Planning and Intelligence," an OIG investigation number, and the month and year that the report was completed. This information is not sensitive and is exactly the type of information often posted on the website of the USCP OIG. (JA-65.)[16]

As far as the contents of the Flash Report, the publicly released version shows that there is an Executive Summary, Background, and Listing of Recommendations. (JA-52-JA-54.) None of these sections contain detailed information about security, policing, or intelligence. The cited deficiencies and proposals to improve security and intelligence discuss the issues only in broad strokes, such as recommending that the USCP "establish policies and procedures designating the specific entity or entities responsible for overseeing the operational planning and execution process for each anticipated event." (JA-44-JA-45.) When the IG discussed this document in his public testimony, he made clear that he did not consider this type of information to be sensitive. (JA-42.) Since the page numbering skips from 2 to 40 and includes an Appendix B, but not an Appendix A,

[16] *Available at* https://www.uscp.gov/the-department/office-inspector-general/audits-investigations

it appears that a vast majority of the document was withheld. The partial release of this document demonstrates that it is possible to segregate and release information of great value to the public while withholding sensitive information, even where the sensitive information may comprise a large portion of the document.

ii. Semiannual Reports

With respect to OIG Semiannual Reports ("SARs"), the First Bolton declaration does not indicate what kind of Security Information is contained in these records or how any such Security Information pertains to one of the categories enumerated in the statute. Instead, the IG declaration simply observes that "Because each SAR is required to include summaries of all work OIG conducted during the preceding six-month period, all categories of reports, whether resulting from audits, investigations, or financial audits, are included in the SAR." (JA-16.) The implication of this statement appears to be that the summaries contained in the SAR incorporate Security Information from audits, investigations, and financial audits. However, the record does not support this implication.

First, even assuming there are individual OIG audits, investigations, or financial audits which constitute Security Information, it does not necessarily follow that *every* Semiannual Report contains a summary of one or more Security Information reports. For example, if no audit, investigation, or financial audit involving Security Information was conducted during a particular six month period, there is

no reason to think that the corresponding Semiannual Report summaries would contain Security Information.

Second, the summaries contained in the Semiannual Reports may be at a level of generality that omits any Security Information. For example, if there was an OIG report which constitutes Security Information because it details the sensitive posting locations for officers, a summary of the OIG's work in the Semiannual Report might simply describe the nature of the USCP's work without identifying those sensitive locations.

Any Security Information contained in the Semiannual Reports is also likely segregable because the reports consist of discrete sections. The contents of Semiannual Reports are specified by 5 U.S.C. § 405(b) (codified at 5 U.S.C. App. 3 § 5(a)(8) at the time of the district court's decision). This provision requires a Semiannual Report to include 22 specific items. While the first Bolton declaration notes that "each SAR is required to include summaries of all work OIG conducted during the preceding six-month period," (JA-16) the 22 items vary widely in terms of their likelihood to constitute Security Information. Neither the First Bolton declaration nor the district court's opinion explain why particular items constitute Security Information as that term is defined in the statute, or even mention specific items.

Examples of information that must be included in the Semiannual Report, but which would not fall within the statutory categories of "policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response" include "statistical tables showing the total number of audit reports, inspection reports, and evaluation reports and the total dollar value of questioned costs," 5 U.S.C. § 405(b)(8) and "a detailed description of any attempt by the establishment to interfere with the independence of the Office, including—(A) with budget constraints designed to limit the capabilities of the Office; and (B) incidents where the establishment has resisted or objected to oversight activities of the Office or restricted or significantly delayed access to information, including the justification of the establishment for such action," 5 U.S.C. § 405(b)(21).

At least one item that must be included in Semiannual Reports does not qualify as Security Information under 2 U.S.C. § 1979(a)(1) because it does not even "relat[e] to Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds." Specifically, "a list of any peer reviews conducted by the Inspector General of another Office of the Inspector General," 5 U.S.C. § 405(b)(16), would contain only information about an agency other than the USCP. Still other information is not sensitive because it is already public, including "a summary of . . . the prosecutions and convictions which have resulted" from referrals to prosecutive authorities. 5 U.S.C. § 405(b)(4). Neither the district court

nor the government explained why sections of the Semiannual Reports containing only non-Security Information could not be released after any Security Information has been redacted.

iii. Financial Audit Reports

With respect to Annual Financial Audit Reports, the First Bolton declaration provides little detail about their contents beyond giving one example of what a hypothetical report "could" recommend: "[A]n audit of OIG's financial statements could recommend stronger internal controls in specified areas, for example, for payroll verification purposes." (JA-16.) However, this description of what the statements "could" contain does not mean that any, much less all, Annual Financial Audit Reports contain this type of information. Moreover, even this hypothetical recommendation regarding payroll verification does not describe information that falls into one of the statutory categories constituting Security Information: "policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response relating to Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds[.]" 2 U.S.C. § 1979(a). Moreover, there is no explanation as to why internal controls for payroll verification purposes would be "sensitive."

While the government did not describe the structure of the annual financial audit reports, Mr. Leopold submitted an excerpt from one publicly available USCP

audit of the agency's budget formulation process. The audit covered "Inadequate Controls," "Past Processes and Practices not Followed," "Overarching Cause 'Tone at the Top,'" "Inaccurate Salaries and Benefits Budget Submissions," and "Potential Shortfall in the Radio Modernization Project." (JA-60). Nothing in the audit appears to contain Security Information. Indeed, commenting on the audit, Rep. Capuano stated, "The issues here have nothing to do with the actual policing of the Hill. . . . . These issues are administrative." *See* Statement of Rep. Capuano, U.S. Capitol Police Budget Concerns: Hearing Before the Subcommittee on Capitol Security, 111 Cong. (2010).

III. The district court erred in concluding that the requesters did not have a statutory right of access to the USCP OIG records.

A. Standard of review

This Court "review[s] questions of statutory construction *de novo*." *Young v. United States*, 943 F.3d 460, 462 (D.C. Cir. 2019).

B. As it existed at the time of the district court's decision, 2 U.S.C. § 1909 required the USCP OIG to publish on its website reports making recommendations for corrective action.

Section 4 of the Inspector General Act of 1978, which was repealed and enacted into positive law after the district court's decision in this case, required that "[i]n carrying out the duties and responsibilities established under this Act, whenever an Inspector General issues a recommendation for corrective action to the agency, the Inspector General . . . not later than 3 days after the recommendation for corrective

action is submitted in final form to the head of the establishment, post the document making a recommendation for corrective action on the website of the Office of Inspector General." 5 U.S.C. App. 3 § 4(e)(1)(C). This provision applied to the USCP IG pursuant to 2 U.S.C. § 1909(c)(1). At the time of the district court's decision, this provision read: "The Inspector General shall carry out the same duties and responsibilities with respect to the United States Capitol Police as an Inspector General of an establishment carries out with respect to an establishment under section 4 of the Inspector General Act of 1978, (5 U.S.C. App. 3 § 4), under the same terms and conditions which apply under such section." The statue has since been amended to replace the reference to section 4 of the Inspector General Act of 1978 with the new location of those statutory provisions in Title 5 of the U.S. Code. P.L. 117-286, 136 Stat. 4196.

A straightforward reading of these statutory provisions requires the Inspector General for the United States Capitol to post to the USCP OIG website a copy of all final recommendations for corrective action within three days after they are submitted. The district court rejected this straightforward reading by citing to *Jam v. Int'l Fin. Corp.*, 139 S. Ct. 759, 769 (2019), a case in which the Supreme Court stated that "a statute that refers to another statute by specific title or section number in effect cuts and pastes the referenced statute as it existed when the referring

statute was enacted, without any subsequent amendments." The Supreme Court called this construction the "reference canon[]." *Id.*

The district court failed to address Mr. Leopold's argument that *Jam* is distinguishable from the present case. The Supreme Court's analysis in *Jam* began by considering the "natural reading" of the statute at issue. The "natural reading," according to the Supreme Court was that "[i]n granting international organizations the 'same immunity' from suit 'as is enjoyed by foreign governments,' the Act seems to continuously link the immunity of international organizations to that of foreign governments, so as to ensure ongoing parity between the two." *Id.* at 768. Only then did the Supreme Court look to the reference canon to "confirm" the natural reading. *Id.* at 769 ("The more natural reading of the IOIA is confirmed by a canon of statutory interpretation that was well established when the IOIA was drafted.") The Supreme Court explained that the IOIA's reference to the immunity "enjoyed by foreign governments" is not to the concept as fixed in 1945, but rather is "an instruction to look up the applicable rules of foreign sovereign immunity, wherever those rules may be found—the common law, the law of nations, or a statute." *Id.* at 770.

The "reference canon" is just that—a canon. It is not to be applied where the language of the statute is unambiguous. *Conn. Nat'l Bank v. Germain*, 503 U.S.

249, 253-54 (1992). ("When the words of a statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'") Thus, while courts may refer to canons of construction to "confirm" that their plain reading of the statute is correct, *Jam*, 139 S. Ct. at 769, they may not use canons of construction to override the plain language of a statute. *See United States v. Chi Ping Patrick Ho*, 984 F.3d 191, 203 (2nd Cir. 2020) ("Nothing in *Jam* compels us to depart from the ordinary meaning of § 1956's clear text or to resort to canons of construction, and we decline to do so today"); *N.Y. ex rel. Office of Children & Family Servs. v. United States HHS Admin. for Children & Families*, 556 F.3d 90, 92 (2nd Cir. 2009) ("Despite the statute's reference to a specific section, we nevertheless understood the text to plainly signal Congress's intent to incorporate the full range of reasonable efforts required by § 671(a)(15)") (cleaned up). As the Seventh Circuit has explained, the reference canon does not create "a categorical rule that compels courts to always read statutory cross-references as pointing to their original targets. Indeed, such a rule would make little sense, as [w]riting a cross-reference rather than repeating the text to be incorporated is useful precisely because the target may be amended. A pointer permits the effect of a change in one section to propagate to other, related, sections without rewriting all of those related sections." *United States v. Head*, 552 F.3d 640, 645-46 (7th Cir. 2009) (internal quotation marks omitted, alteration in original).

Here, the plain and natural reading of 2 U.S.C. § 1909(c)(1), as it existed at the time of the district court's decision, is that changes to the powers and duties of inspectors general under the Inspector General Act of 1978 would apply to the USCP IG as well. The USCP OIG statue provided that "[t]he Inspector General shall carry out the same duties and responsibilities . . . under the same terms and conditions which apply under such section [5 U.S.C. App. 4]." Thus, the two sections were explicitly linked with language that ensured there would be no differences between how 5 U.S.C. App. 3 § 4 operated with respect to the U.S. Capitol Police and executive branch establishments. Indeed, the title of the subsection was "Applicability of duties of Inspector General of executive branch establishment." The "same duties and responsibilities" and "same terms and conditions" language in 2 U.S.C. § 1909(c)(1), which has not been altered since the district court's decision, is indistinguishable from the language in the statute at issue in *Jam*, which the Supreme Court found to require the referring statute to incorporate future changes in the law: "The language of the IOIA more naturally lends itself to petitioners' reading. In granting international organizations the 'same immunity' from suit 'as is enjoyed by foreign governments,' the Act seems to continuously link the immunity of international organizations to that of foreign governments, so as to ensure ongoing parity between the two." 139 S.Ct. at 768.

C. Recent statutory changes confirm that Congress intended amendments to the Inspector General Act of 1978 to propagate to the U.S. Capitol Police organic statute.

During the course of this appeal, Congress enacted "An Act To make revisions in title 5, United States Code, as necessary to keep the title current, and to make technical amendments to improve the United States Code." P.L. 117-286, 136 Stat. 4196 (hereinafter "the Act"). This Act codified the Inspector General Act of 1978 into positive law in Title 5 of the U.S. Code. It did so by repealing portions of P.L. 95-452, 92 Stat. 1101 (Inspector General Act of 1978) and P.L. 110-409, 122 Stat. 4302 (Inspector General Reform Act of 2008) in Section 7 of the Act ("Repeals," Schedule of Laws Repealed) and amending Title 5 to include a new Chapter 4 containing the substance of the repealed provisions. P.L. 117-286 § 3(b), 136 Stat. 4196 § 3(b). Conforming changes were made to Section 1004 of the Legislative Branch Appropriations Act, 2006, P.L. 109-55, 119 Stat. 565 (codified at 2 U.S.C. § 1909), which established the Office of the Inspector General for the United States Capitol Police. P.L. 117-286 § 4(b)(4), 136 Stat. 4196 § 4(b)(4). The conforming changes updated references to the Inspector General Act of 1978 with references to the new positive law provisions. *Id.*

The current version of 2 U.S.C. § 1909(c)(1) refers to the USCP IG as having the same "duties and responsibilities as . . . an establishment under section 404 of title 5, United States Code," rather than "section 4 of the Inspector General Act of

1978, (5 U.S.C. App. 4)[.]" Under the parlance of the new Act, 2 U.S.C. § 1909(c)(1) is now said to contain a reference to a "restated provision," which means "a provision of title 5, United States Code, that is enacted by section 3." P.L. 117-286 § 5(a)(1), 136 Stat. 4196 § (5)(a)(1).The new Act prescribes that "[a] reference to a restated provision is deemed to refer to the corresponding source provision." P.L. 117-286 § 5(d), 136 Stat. 4196 § (5)(d). A "source provision" is "a provision of law that is replaced by a restated provision." P.L. 117-286 § 5(a)(2), 136 Stat. 4196 § (5)(a)(2). Here, the provision of law that was replaced is section 4 of the Inspector General Act of 1978 as it existed on October 19, 2021, the "cutoff date" provided in the new Act. P.L. 117-286 § 5(b), 136 Stat. 4196 § (5)(b) ("The restated provisions replace certain provisions of law enacted on or before October 19, 2021.") That provision makes it further evident that Congress intended to bring all references to the source provisions up to date and for such references to be interpreted dynamically in the future: "If a law enacted after that date amends or repeals a source provision, that law is deemed to amend or repeal, as the case may be, the corresponding restated provision." P.L. 117-286 § 5(b), 136 Stat. 4196 § (5)(b).

Since the Act was not intended to make any changes to substantive law, but simply to provide clarification, it follows that the Act was merely confirming what

was already the case—that changes to the IG Act were incorporated into the U.S. Capitol Police organic statute.

CONCLUSION

For the foregoing reasons, this Court should reverse the district court's order dismissing the case for lack of subject matter jurisdiction and remand for further proceedings.

Respectfully Submitted,

/s/ Jeffrey Light
Jeffrey L. Light
D.C. Bar #485360
1629 K St., NW
Suite 300
Washington, DC 20006
(202)277-6213
Jeffrey@LawOfficeOfJeffreyLight.com

Counsel for Plaintiff-Appellant

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

I certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because the brief contains 12,809 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

I certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. R. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Office 365 in 14-point Times New Roman.

_/s/ Jeffrey Light_____
Jeffrey Light

CERTIFICATE OF SERVICE

I hereby certify that on April 18, 2023, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users and service will be accomplished by the appellate CM/ECF system.

_/s/ Jeffrey Light_____
Jeffrey Light

ADDENDUM

Table of Contents

2 U.S.C. § 1909

(a) Establishment of Office. There is established in the United States Capitol Police the Office of the Inspector General (hereafter in this section referred to as the "Office"), headed by the Inspector General of the United States Capitol Police (hereafter in this section referred to as the "Inspector General").

(b) Inspector General.

(1) Appointment. The Inspector General shall be appointed by, and under the general supervision of, the Capitol Police Board. The appointment shall be made in consultation with the Inspectors General of the Library of Congress, Government Printing Office, and the Government Accountability Office. The Capitol Police Board shall appoint the Inspector General without regard to political affiliation and solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations.

(2) Term of service. The Inspector General shall serve for a term of 5 years, and an individual serving as Inspector General may be reappointed for not more than 2 additional terms.

(3) Removal. The Inspector General may be removed from office prior to the expiration of his term only by the unanimous vote of all of the voting members of the Capitol Police Board, and the Board shall communicate the reasons for any such removal to the Committee on House Administration, the Senate Committee on Rules and Administration and the Committees on Appropriations of the House of Representatives and of the Senate.

(4) Salary. The Inspector General shall be paid at an annual rate equal to $1,000 less than the annual rate of pay in effect for the Chief of the Capitol Police.

(5) Deadline. The Capitol Police Board shall appoint the first Inspector General under this section not later than 180 days after the date of the enactment of this Act.

(c) Duties.

(1) Applicability of duties of Inspector General of executive branch establishment. The Inspector General shall carry out the same duties and responsibilities with respect to the United States Capitol Police as an Inspector General of an establishment carries out with respect to an establishment under

section 404 of title 5, United States Code, under the same terms and conditions which apply under such section.

(2) Semiannual reports. The Inspector General shall prepare and submit semiannual reports summarizing the activities of the Office in the same manner, and in accordance with the same deadlines, terms, and conditions, as an Inspector General of an establishment under section 405 (other than subsection (b)(13) thereof) of title 5, United States Code. For purposes of applying section 405 of such title to the Inspector General, the Chief of the Capitol Police shall be considered the head of the establishment. The Chief shall, within 30 days of receipt of a report, report to the Capitol Police Board, the Committee on House Administration, the Senate Committee on Rules and Administration, and the Committees on Appropriations of the House of Representatives and of the Senate consistent with section 405(c) of such title.

(3) Investigations of complaints of employees and members.

(A) Authority. The Inspector General may receive and investigate complaints or information from an employee or member of the Capitol Police concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety, including complaints or information the investigation of which is under the jurisdiction of the Internal Affairs Division of the Capitol Police as of the date of the enactment of this Act.

(B) Nondisclosure. The Inspector General shall not, after receipt of a complaint or information from an employee or member, disclose the identity of the employee or member without the consent of the employee or member, unless required by law or the Inspector General determines such disclosure is otherwise unavoidable during the course of the investigation.

(C) Prohibiting retaliation. An employee or member of the Capitol Police who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee or member as a reprisal for making a complaint or disclosing information to the Inspector General, unless the complaint was made or the information disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(4) Independence in carrying out duties. Neither the Capitol Police Board, the Chief of the Capitol Police, nor any other member or employee of the Capitol Police may prevent or prohibit the Inspector General from carrying out any of

the duties or responsibilities assigned to the Inspector General under this section.

(d) Powers.

(1) In general. The Inspector General may exercise the same authorities with respect to the United States Capitol Police as an Inspector General of an establishment may exercise with respect to an establishment under section 406(a) of title 5, United States Code, other than paragraphs (7) and (8) of such section.

(2) Staff.

(A) In general. The Inspector General may appoint and fix the pay of such personnel as the Inspector General considers appropriate. Such personnel may be appointed without regard to the provisions of title 5, United States Code, regarding appointments in the competitive service, and may be paid without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no personnel of the Office (other than the Inspector General) may be paid at an annual rate greater than $500 less than the annual rate of pay of the Inspector General under subsection (b)(4).

(B) Experts and consultants. The Inspector General may procure temporary and intermittent services under section 3109 of title 5, United States Code, at rates not to exceed the daily equivalent of the annual rate of basic pay for level IV of the Executive Schedule under section 5315 of such title.

(C) Independence in appointing staff. No individual may carry out any of the duties or responsibilities of the Office unless the individual is appointed by the Inspector General, or provides services procured by the Inspector General, pursuant to this paragraph. Nothing in this subparagraph may be construed to prohibit the Inspector General from entering into a contract or other arrangement for the provision of services under this section.

(D) Applicability of Capitol Police personnel rules. None of the regulations governing the appointment and pay of employees of the Capitol Police shall apply with respect to the appointment and compensation of the personnel of the Office, except to the extent agreed to by the Inspector General. Nothing in the previous sentence may be construed to affect subparagraphs (A) through (C).

(3) Equipment and supplies. The Chief of the Capitol Police shall provide the Office with appropriate and adequate office space, together with such

equipment, supplies, and communications facilities and services as determined by the Inspector General to be necessary for the operation of the Office, and shall provide necessary maintenance services for such office space and the equipment and facilities located therein.

(e) Transfer of functions.

(1) Transfer. To the extent that any office or entity in the Capitol Police prior to the appointment of the first Inspector General under this section carried out any of the duties and responsibilities assigned to the Inspector General under this section, the functions of such office or entity shall be transferred to the Office upon the appointment of the first Inspector General under this section.

(2) No reduction in pay or benefits. The transfer of the functions of an office or entity to the Office under paragraph (1) may not result in a reduction in the pay or benefits of any employee of the office or entity, except to the extent required under subsection (d)(2)(A).

(f) Effective date. This section shall be effective upon enactment of this Act.

2 U.S.C. § 1979

(a) Definition. In this section, the term "security information" means information that—

(1) is sensitive with respect to the policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response relating to Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds; and

(2) is obtained by, on behalf of, or concerning the Capitol Police Board, the Capitol Police, or any incident command relating to emergency response.

(b) Authority of Board to determine conditions of release. Notwithstanding any other provision of law, any security information in the possession of the Capitol Police may be released by the Capitol Police to another entity, including an individual, only if the Capitol Police Board determines in consultation with other appropriate law enforcement officials, experts in security preparedness, and appropriate committees of Congress, that the release of the security information will not compromise the security and safety of the Capitol buildings and grounds or any individual whose protection and safety is under the jurisdiction of the Capitol Police.

(c) Rule of construction. Nothing in this section may be construed to affect the ability of the Senate and the House of Representatives (including any Member, officer, or committee of either House of Congress) to obtain information from the Capitol Police regarding the operations and activities of the Capitol Police that affect the Senate and House of Representatives.

(d) Regulations. The Capitol Police Board may promulgate regulations to carry out this section, with the approval of the Committee on Rules and Administration of the Senate and the Committee on House Administration of the House of Representatives.

(e) Effective date. This section shall take effect on the date of enactment of this Act and apply with respect to—

(1) any remaining portion of fiscal year 2004, if this Act is enacted before October 1, 2004; and

(2) fiscal year 2005 and each fiscal year thereafter.

5 U.S.C. § 405

(a) Definitions. In this section:

(1) Disallowed cost. The term "disallowed cost" means a questioned cost that management, in a management decision, has sustained or agreed should not be charged to the Government.

(2) Final action. The term "final action" means—

(A) the completion of all actions that the management of an establishment has concluded, in its management decision, are necessary with respect to the findings and recommendations included in an audit report; and

(B) in the event that the management of an establishment concludes no action is necessary, final action occurs when a management decision has been made.

(3) Management decision. The term "management decision" means the evaluation by the management of an establishment of the findings and recommendations included in an audit report and the issuance of a final decision by management concerning its response to the findings and recommendations, including actions concluded to be necessary.

(4) Questioned cost. The term "questioned cost" means a cost that is questioned by the Office because of—

(A) an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds;

(B) a finding that, at the time of the audit, the cost is not supported by adequate documentation; or

(C) a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

(5) Recommendation that funds be put to better use. The term "recommendation that funds be put to better use" means a recommendation by the Office that funds could be used more efficiently if management of an establishment took actions to implement and complete the recommendation, including—

(A) reductions in outlays;

(B) deobligation of funds from programs or operations;

(C) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds;

(D) costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor, or grantee;

(E) avoidance of unnecessary expenditures noted in preaward reviews of contract or grant agreements; or

(F) any other savings which are specifically identified.

(6) Senior Government employee. The term "senior Government employee" means—

(A) an officer or employee in the executive branch (including a special Government employee as defined in section 202 of title 18 [18 USCS § 202]) who occupies a position classified at or above GS-15 of the General Schedule or, in the case of positions not under the General Schedule, for which the rate of basic pay is equal to or greater than 120 percent of the minimum rate of basic pay payable for GS-15 of the General Schedule; and

(B) any commissioned officer in the Armed Forces in pay grades O-6 and above.

(7) Unsupported cost. The term "unsupported cost" means a cost that is questioned by the Office because the Office found that, at the time of the audit, such cost is not supported by adequate documentation.

(b) Semiannual reports. Each Inspector General shall, not later than April 30 and October 31 of each year, prepare semiannual reports summarizing the activities of the Office during the immediately preceding 6-month periods ending March 31 and September 30. The reports shall include, but need not be limited to—

(1) a description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of such establishment disclosed by such activities during the reporting period;

(2) a description of the recommendations for corrective action made by the Office during the reporting period with respect to significant problems, abuses, or deficiencies identified pursuant to paragraph (1);

(3) an identification of each significant recommendation described in previous semiannual reports on which corrective action has not been completed;

(4) a summary of matters referred to prosecutive authorities and the prosecutions and convictions which have resulted;

(5) a summary of each report made to the head of the establishment under section 406(c)(2) of this title [5 USCS § 406(c)(2)] during the reporting period;

(6) a listing, subdivided according to subject matter, of each audit report, inspection report, and evaluation report issued by the Office during the reporting period and for each report, where applicable, the total dollar value of questioned costs (including a separate category for the dollar value of unsupported costs) and the dollar value of recommendations that funds be put to better use;

(7) a summary of each particularly significant report;

(8) statistical tables showing the total number of audit reports, inspection reports, and evaluation reports and the total dollar value of questioned costs (including a separate category for the dollar value of unsupported costs), for reports—

(A) for which no management decision had been made by the commencement of the reporting period;

(B) which were issued during the reporting period;

(C) for which a management decision was made during the reporting period, including—

(i) the dollar value of disallowed costs; and

(ii) the dollar value of costs not disallowed; and

(D) for which no management decision has been made by the end of the reporting period;

(9) statistical tables showing the total number of audit reports, inspection reports, and evaluation reports and the dollar value of recommendations that funds be put to better use by management, for reports—

(A) for which no management decision had been made by the commencement of the reporting period;

(B) which were issued during the reporting period;

(C) for which a management decision was made during the reporting period, including—

(i) the dollar value of recommendations that were agreed to by management; and

(ii) the dollar value of recommendations that were not agreed to by management; and

(D) for which no management decision has been made by the end of the reporting period;

(10) a summary of each audit report, inspection report, and evaluation report issued before the commencement of the reporting period—

(A) for which no management decision has been made by the end of the reporting period (including the date and title of each such report), an explanation of the reasons such management decision has not been made, and a statement concerning the desired timetable for achieving a management decision on each such report;

(B) for which no establishment comment was returned within 60 days of providing the report to the establishment; and

(C) for which there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations;

(11) a description and explanation of the reasons for any significant revised management decision made during the reporting period;

(12) information concerning any significant management decision with which the Inspector General is in disagreement;

(13) the information described under section 804(b) of the Federal Financial Management Improvement Act of 1996 (Public Law 104-208, Sec. 101(f) [title VIII], 31 U.S.C. 3512 note);

(14)

(A) an appendix containing the results of any peer review conducted by another Office of Inspector General during the reporting period; or

(B) if no peer review was conducted within that reporting period, a statement identifying the date of the last peer review conducted by another Office of Inspector General;

(15) a list of any outstanding recommendations from any peer review conducted by another Office of Inspector General that have not been fully implemented, including a statement describing the status of the implementation and why implementation is not complete;

(16) a list of any peer reviews conducted by the Inspector General of another Office of the Inspector General during the reporting period, including a list of any outstanding recommendations made from any previous peer review (including any peer review conducted before the reporting period) that remain outstanding or have not been fully implemented;

(17) statistical tables showing—

(A) the total number of investigative reports issued during the reporting period;

(B) the total number of persons referred to the Department of Justice for criminal prosecution during the reporting period;

(C) the total number of persons referred to State and local prosecuting authorities for criminal prosecution during the reporting period; and

(D) the total number of indictments and criminal informations during the reporting period that resulted from any prior referral to prosecuting authorities;

(18) a description of the metrics used for developing the data for the statistical tables under paragraph (17);

(19) a report on each investigation conducted by the Office involving a senior Government employee where allegations of misconduct were substantiated, including the name of the senior government official (as defined by the department or agency) if already made public by the Office, and a detailed description of—

(A) the facts and circumstances of the investigation; and

(B) the status and disposition of the matter, including—

(i) if the matter was referred to the Department of Justice, the date of the referral; and

(ii) if the Department of Justice declined the referral, the date of the declination;

(20)

(A) a detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation; and

(B) what, if any, consequences the establishment actually imposed to hold the official described in subparagraph (A) accountable;

(21) a detailed description of any attempt by the establishment to interfere with the independence of the Office, including—

(A) with budget constraints designed to limit the capabilities of the Office; and

(B) incidents where the establishment has resisted or objected to oversight activities of the Office or restricted or significantly delayed access to

information, including the justification of the establishment for such action; and

(22) detailed descriptions of the particular circumstances of each—

(A) inspection, evaluation, and audit conducted by the Office that is closed and was not disclosed to the public; and

(B) investigation conducted by the Office involving a senior Government employee that is closed and was not disclosed to the public.

(c) Furnishing semiannual reports to head of establishment and Congress. Semiannual reports of each Inspector General shall be furnished to the head of the establishment involved not later than April 30 and October 31 of each year and shall be transmitted by the head of the establishment to the appropriate committees or subcommittees of the Congress within 30 days after receipt of the report, together with a report by the head of the establishment containing—

(1) any comments the head of the establishment determines appropriate;

(2) statistical tables showing the total number of audit reports, inspection reports, and evaluation reports and the dollar value of disallowed costs, for reports—

(A) for which final action had not been taken by the commencement of the reporting period;

(B) on which management decisions were made during the reporting period;

(C) for which final action was taken during the reporting period, including—

(i) the dollar value of disallowed costs that were recovered by management through collection, offset, property in lieu of cash, or otherwise; and

(ii) the dollar value of disallowed costs that were written off by management; and

(D) for which no final action has been taken by the end of the reporting period;

(3) statistical tables showing the total number of audit reports, inspection reports, and evaluation reports and the dollar value of recommendations that funds be put to better use by management agreed to in a management decision, for reports—

(A) for which final action had not been taken by the commencement of the reporting period;

(B) on which management decisions were made during the reporting period;

(C) for which final action was taken during the reporting period, including—

(i) the dollar value of recommendations that were actually completed; and

(ii) the dollar value of recommendations that management has subsequently concluded should not or could not be implemented or completed; and

(D) for which no final action has been taken by the end of the reporting period;

(4) whether the establishment entered into a settlement agreement with the official described in subsection (b)(20)(A), which shall be reported regardless of any confidentiality agreement relating to the settlement agreement; and

(5) a statement with respect to audit reports on which management decisions have been made but final action has not been taken, other than audit reports on which a management decision was made within the preceding year, containing—

(A) a list of such audit reports and the date each such report was issued;

(B) the dollar value of disallowed costs for each report;

(C) the dollar value of recommendations that funds be put to better use agreed to by management for each report; and

(D) an explanation of the reasons final action has not been taken with respect to each audit report, except that the statement may exclude any audit reports that are under formal administrative or judicial appeal or upon which management of an establishment has agreed to pursue a legislative solution, but the statement shall identify the number of reports in each category so excluded.

(d) Reports available to public. Within 60 days of the transmission of the semiannual reports of each Inspector General to Congress, the head of each establishment shall make copies of the report available to the public upon request and at a reasonable cost. Within 60 days after the transmission of the semiannual reports of each establishment head to Congress, the head of each establishment shall make copies of the report available to the public upon request and at a reasonable cost.

(e) Reporting serious problems, abuses, or deficiencies. Each Inspector General shall report immediately to the head of the establishment involved whenever the Inspector General becomes aware of particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs and operations of the establishment. The head of the establishment shall transmit any such report to the appropriate committees or subcommittees of Congress within 7 calendar days,

together with a report by the head of the establishment containing any comments the establishment head deems appropriate.

(f) Limitation on public disclosure of information.

(1) In general. Nothing in this section shall be construed to authorize the public disclosure of information that is—

(A) specifically prohibited from disclosure by any other provision of law;

(B) specifically required by Executive order to be protected from disclosure in the interest of national defense or national security or in the conduct of foreign affairs; or

(C) a part of an ongoing criminal investigation.

(2) Criminal investigation information in public records. Notwithstanding paragraph (1)(C), any report under this section may be disclosed to the public in a form which includes information with respect to a part of an ongoing criminal investigation if such information has been included in a public record.

(3) No authorization to withhold information from Congress. Except to the extent and in the manner provided under section 6103(f) of the Internal Revenue Code of 1986 (26 U.S.C. 6103(f)), nothing in this section or in any other provision of this chapter [5 USCS §§ 401 et seq.] shall be construed to authorize or permit the withholding of information from Congress, or from any committee or subcommittee of Congress.

(4) Provision of information to members of Congress. Subject to any other provision of law that would otherwise prohibit disclosure of such information, the information described in paragraph (1) may be provided to any Member of Congress upon request.

(5) Protection of personally identifiable information of whistleblowers. An Office may not provide to Congress or the public any information that reveals the personally identifiable information of a whistleblower under this section unless the Office first obtains the consent of the whistleblower.